

EXHIBIT 39



5/21/20: i

@solarwinds

SolarWinds Scorecard

NIST Maturity Level



Steady progress in 1H. On track for 2020 Improvement

Security Category	2017	2018	2019	2020 Target	Key Risks	1H 2020 Improvement Plan
Identify	0.8	2.0	3.0	↑3.3	• Security processes not consistently implemented	• Increase SDL adoption • Advance product certifications
Protect	1.5	3.0	3.2	↑3.3	• Significant deficiencies in user access management	• Enforce AD Authentication for critical systems
Detect	1.0	2.8	3.4	↑3.6	• Inconsistent security scanning	• Expand and standardize VAT, Pen, Open Source, and Code Analysis
Respond	0.8	2.8	3.6	↑3.8	• Increase in events and complexity	• Continuous improvements in Security Major Incident Response
Recover	0.7	2.0	2.0	↑2.3	• Immature business continuity plan	• Operational Continuity Plan assessment and improvements
Overall	1.0	2.5	3.0	↑3.3		

Maturity	Description
0	No evidence
1	Reactive approach
2	Consistent approach, Somewhat reactive and undocumented
3	Documented, detailed approach. Regularly measure its compliance
4	Established risk management framework
5	Refined practice, focused on improvements and efficiencies

CONFIDENTIAL - NOT FOR DISTRIBUTION © 2020 SolarWinds Worldwide, LLC. All rights reserved.

@solarwinds

4

@solarwinds

Q1 2020 AD Access Audit Deficiency | Remediation



solarwinds

ROOT CAUSE ANALYSIS (RCA)

PRELIMINARY ROOT CAUSE ANALYSIS (RCA) Active Directory Access Review Audit Deficiency (SOX ITGC)

DEVELOPMENT, OPERATIONS & INFORMATION TECHNOLOGY

Incident Date: Q1 2020 Affected Service: SOX ITGC Severity: TRO - Control Deficiency

Incident Summary

The Q1-2020 Sarbanes Oxley (SOX) Information Technology General Controls (ITGC) stipulate that user privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory users) and databases.

During the Q1-2020 external audit of Active Directory on 5/4/2020, PwC auditors and Internal Audit determined the AD Q1 audit did not sufficiently answer the objective, as it was unclear if AD users were active and that their access was appropriate.

During the RCA investigation, two major breakdowns are attributed to 1) inconsistent data for contractors and vendors and the need for a single source of truth and 2) the overall AD Audit review process did not meet the audit objectives. These breakdowns created risk of unauthorized users having in appropriate access to AD.

As a result of the RCA, the following corrective actions have been immediately implemented:

- Vendors and Contractors have been consolidated into a single, centrally managed list and a process has been established for hiring managers to request, change and/or remove AD access.
- The Service Desk team has reviewed 343 individuals, identified during the first audit as requiring validating and rerun the audit, with May information to affirm appropriate access has been established.
- The Service Desk team identified 18 additional individuals who were identified as active, however were inactive contractors and/or vendors.

In addition to these immediate steps, there are plans to automate the audit process, and incorporate vendors and contractors into the HRIS system (est. 2021).

Root Cause

The ITGC Q1-2020 User Access Review for AD failed due to incomplete data and an incomplete audit process, as outlined below:

No.	Issue	AD User Access Management (ITGC)	Root Cause	Impact
1	Inconsistent Vendor and Contractor Data	The Vendor and Contract lists, used to evaluate the AD UAR data, was incomplete.	No single, authoritative source of truth	Audit failure due to incomplete lists resulted in the appearance of 325 users, potentially having inappropriate access to AD.
2	Audit Processes do not meet audit objective	The AD UAR was unable to demonstrate if AD users were active and/or if active, if their access was appropriate.	Process design did not meet audit objectives	Audit failure due to processes not adequately demonstrating objective.

CONFIDENTIAL

	Authorized	Unauthorized	Grand Total
Employee in Updated List	198	9	207
SolarPeople	132		132
Vendor List - Flexis	18		18
SolarPeople - Intern	11	2	13
Contractor List - Mina	12		12
Vendor	11	1	12
Vendor List - Michal	8		8
Contractor	6	1	7
No Show Day 1 - No SARF Term Received		3	3
No SARF Term Received		1	1
SARF Term Sent Late		1	1
Timing Issue	14		14
SARF Term	7		7
New Hire	7		7
Not on Managed List	83	21	104
Vendor	53	1	54
Contractor	18	9	27
M&A	12	2	14
Unknown		6	6
Employee		3	3
Erroneously excluded from audit		18	21
Grand Total	295	48	343

Key Corrective Actions

- Created authoritative list of vendors and contractors
- Redefined audit procedures

@solarwinds 17

@solarwinds